Claims

1. A method for marking an electronic document as a valid document comprising the steps of:
   a) examining a digital signature associated with the document,
   b) examining the structure associated with the document, and
   wherein if the steps examining the digital signature and the structure associated with the document determine that the signature and structure are valid for that document then the document is marked as a valid document, and if either of the steps of examining the digital signature or the structure determine that the digital signature or structure are not valid for that document, then the other of the steps of examining the digital signature or structure is terminated prior to concluding whether that step is valid, and the document is marked as an invalid document.

2. The method as claimed in claim 1 wherein the step of examining the digital signature comprises the steps of:
   a) extracting a digital signature from the document,
   b) determining whether the signature references a digital certificate and returning a valid response if the signature references a digital certificate, and if the signature does not reference a digital certificate terminating the examination of the signature and structure.

3. The method as claimed in claim 2 further comprising the steps of:

a) on receiving a valid response from the
    determination of whether the signature references
    a certificate, determining whether the
    certificate is a valid certificate, and

5 b) on confirming that the signature references a
    certificate and the certificate is a valid
    certificate marking the signature as being
    validly confirmed.

10 4. The method as claimed in claim 3 wherein the step of
    examining the digital signature further includes the
    step of:

a) marking the signature as invalid if the step of
    determining whether the certificate is a valid
15   certificate fails, and terminating the
    examination of the signature and structure.

20 5. The method as claimed in claim 2 or claim 4 wherein
    the step of terminating the examination of the
    signature and structure comprises the step of flagging
    a shared memory location within a computer processor
    so as to effect a marking within the shared memory
    location that the examination of the signature has
25 failed.

30 6. The method as claimed in any preceding claim wherein
    the step of examining the document structure comprises
    the steps of:

a) determining if the document is structurally
    valid, and

b) determining if the document is syntactically
    valid.

7.   The method as claimed in claim 6 wherein the step of
     determining if the document is structurally valid
     comprises the steps of:
     a)   extracting information from the document relating
          to the structure of the document,
     b)   comparing the extracted information against a
          series of stored rules so as to determine whether
          the extracted information matches the stored
          information, and
     c)   on determining that the extracted information
          matches the stored information marking the
          document as structurally valid.

8.   The method as claimed in claim 6 wherein the step of
     determining if the document is syntactically valid
     comprises the steps of:
     a)   extracting information from the document relating
          to the syntax of the document,
     b)   comparing the extracted information against a
          series of stored rules so as to determine whether
          the extracted information matches the stored
          information, and
     c)   on determining that the extracted information
          matches the stored information marking the
          document as syntactically valid.

9.   The method as claimed in claim 7 wherein on
     determining that the document is not structurally
     valid comprises the performing the additional step of:
     a)   flagging a shared memory location with a marker
          so as to identify that the structure has been
          found invalid.

10. The method as claimed in claim 8 wherein on
     determining that the document is not syntactically

valid comprises the performing the performing the
additional step of:

a)   flagging a shared memory location with a marker
     so as to identify that the syntax has been found
     invalid.

11. The method as claimed in claim 9 wherein the marking
     of the shared memory location with a marker so as to
     identify that the structure has been found invalid
     effects a termination of the examination of the
     digital signature and the document structure.

12. The method as claimed in claim 10 wherein the marking
     of the shared memory location with a marker so as to
     identify that the syntax has been found invalid
     effects a termination of the examination of the
     digital signature and the document structure.

13. The method as claimed in claim 1 wherein a shared
     memory location is accessed during both of the steps
     of examining the signature and examining the document
     structure, the noting of a marked failure within the
     shared memory effecting a termination of the
     examination of the signature or the document
     structure.

14. The method as claimed in claim 13 wherein the noting
     of a marked failure within the shared memory location
     is effected by incrementing or decrementing a value
     stored within the shared memory location, and on
     accessing the shared memory location any deviation
     between the actual value measured at the shared memory
     location and a previously measured value results in a
     termination of the examination of the signature or the
     document structure.

15. The method as claimed in claim 1 wherein the steps of examining the document signature and the document structure are conducted as multiple threads within the same process.

16. A computer system adapted for the concurrent processing of digitally signed document, the system comprising:

    a)   a signature verification module adapted to verify the signature associated with a document,

    b)   a document structure verification module adapted to verify the structure of a document,

    c)   a state processor, and

wherein both the signature verification module and the document structure verification module interface with the state processor during verification of the signature and verification of the document structure, and wherein the state processor is adapted in response to a verification failure of either the signature or structure to flag the failure and wherein the signature verification module and the document structure verification module are adapted to terminate verification upon detection of the failure flag arising from the failure of the other verification process.